

## Chinese Judicial Authorities Issue Interpretation on Criminal Liability for Misuse of Personal Information

*Official guidance has expanded the scope of laws and provided examples of illegal uses.*

### Key Points:

- The definition of “personal information” has been expanded to include data points used for tracking individuals through trails of activity.
- Certain misconduct by companies or individuals that breaches the Network Security Law with aggravating circumstances may lead to criminal liability including imprisonment of up to seven years and/or an unspecified fine.
- Aggravating circumstances for criminal offenses have also been clarified.

On May 9, 2017, the Supreme People’s Court of China (SPC) and the Supreme People’s Procuratorate (SPP) published a Judicial Interpretation on Infringing Personal Information (the Interpretation), providing guidance on criminal penalties for the misuse of personal information under the Chinese Criminal Law. This guidance has been issued in relation to amendments to the Criminal Law made in 2015 and will directly affect how the Network Security Law (NSL), which comes into effect on 1 June 2017, will be interpreted by the authorities.

The Interpretation is significant because it: (i) expands the scope of the definition of “personal information” (ii) sets out potential criminal liabilities for companies and individuals that mishandle personal information; (iii) provides examples of illegal use and disclosure of personal information and (iv) clarifies certain aggravating conditions that could result in a Criminal penalty under Chinese criminal law.

On the same day, the SPC, the SPP and the Ministry of Public Security held a rare joint press conference to provide additional background and context about the Interpretation. During the press conference, the judicial authorities and enforcement agencies illustrated through case studies how the Interpretation should be used to provide guidance on non-compliance with both laws.

### Background

The Criminal Law in China imposes penalties (of up to seven years imprisonment) and/or fines (of an unspecified amount) on any individual and/or entity that, in violation of the relevant laws sells or discloses personal information to a third party or steals or uses other means to illegally obtain personal information. The Criminal Law states that individuals who sell or disclose personal information that was obtained during the course of discharging duties or providing services shall be subject to harsher criminal penalties.

The opinions expressed in the Interpretation regarding the application of the Criminal Law to breaches of the new NSL escalate the administrative penalties imposed under the NSL to the criminal liability under the Criminal Law for the most severe offenses. Any individual and/or entity may face criminal penalties of up to three years in prison and/or a criminal fine if that party: (i) fails to comply with legal and regulatory obligations to properly maintain information network security; (ii) refuses to rectify any noncompliance as ordered by regulatory authorities; or (iii) leaks personal information.

Since the criminal penalties may apply to individuals and entities, it is possible that there could be a situation involving corporate criminal liability for a company as well as for those supervisors and employees directly involved.

## Interpretation Guidance

- Scope of Personal Information definition expanded: The Interpretation expands the scope of personal information to include data points used for tracking individuals through trails of activity. It defines personal information as any information that “is recorded in digital or other means, and can, individually or collectively, identify individuals or reflect activities of individuals, including but not limited to name, identification number, contact details, address, account and password, financial conditions and trace records.” Examples of these “activity trails” of personal information are registration information, mobile location, accommodation records, credit records, education information and online shopping information, among others.
- Guidance on Failure to Maintain Security: The Interpretation states that any network service provider (a term that is not defined in either the NSL or the Criminal Law) that fails to maintain the security of information networks in accordance with law (including the NSL) and that refuses to take measures to rectify non-compliance as ordered by regulatory authorities shall be sentenced to imprisonment for up to three years and/or face an unspecified criminal fine. This does not apply to “network operators” which as defined under the NSL include not only network service providers, but also network owners and administrators. This is likely a gap in the Criminal Law and the NSL that only network service providers are subject to the criminal penalties, as the latter was passed a year after the latest amendments to the former.
- Examples of “Illegally Providing and Obtaining Personal Information”: The Interpretation states that under the Criminal Law providing personal information to any third party, as well as publishing personal information online or by any other means shall be viewed as “providing [a] citizen’s personal information.” It further indicates that providing lawfully collected personal information to any third party without the data subject’s consent also falls within the scope of “providing personal information,” unless such personal information has been anonymized in such a way that personal details cannot be recovered. Furthermore, the Interpretation provides that purchasing, receiving and exchanging personal information in a manner violating Chinese laws and regulations, or illegally collecting information when performing duties or providing services, for example through hacking a website, should be viewed as “illegally obtaining personal information.”
- Clarification of Aggravated Circumstances: The Criminal Law in China also states that an offender whose actions include “Serious Circumstances” (as defined below) may be sentenced for up to three years in prison. An offender with “Extremely Serious Circumstances” (also defined below) may be sentenced to imprisonment for up to seven years. The Interpretation further clarifies both sets of circumstances, as outlined below.

- Serious Circumstances include any of the following circumstances which arise in respect of personal information:
  - i. The intention of selling or providing the personal information is to commit other crimes
  - ii. There is a high quantity or value threshold for the following types of illegally obtained personal information, including :
    - 1. 50 pieces of information about location data, communications content, credit records and financial data
    - 2. 500 pieces of information about whereabouts, communication records, health and biologic information, transaction records and other information involving personal and financial security
    - 3. 5,000 pieces of other personal information
    - 4. The cumulative quantity of data has reached the imposed threshold; or
    - 5. A value of RMB5,000 (approximately US\$727) or more of illegal gains from selling/ processing etc the data
  - iii. If the personal information is collected during the course of performing duties or providing service, the quantitative thresholds of information or illegal gain can be further lowered to 50% of the figures enumerated in (ii)
  - iv. repeated offenses, with previous criminal records or within two years of an administrative penalty for misuse of personal information

The Interpretation makes a distinction between the personal information outside of the types of personal information noted in (ii)(2) and (ii)(3) when considering Serious Circumstances. The Interpretation notes that when an individual or company, for lawful business activities, illegally purchases or receives the personal information not within the categories of (ii)(2) and (ii)(3) above, the monetary threshold shall be increased to RMB50,000 (approximately US\$7,279) or more in terms of the value of the illegal gain.

- Extremely Serious Circumstances are defined in the Interpretation as circumstances which result in any of the following:
  - i. Death, serious injury, lunacy or kidnapping of victims
  - ii. Significant economic loss or severe social influence
  - iii. At least 10 times of the quantities of personal information specified in Serious Circumstances

## Conclusion

Overall, the Interpretation expands the definition of personal information and provides clearer detail about the circumstances of infringement and the aggravating circumstances that may lead to criminal penalties on companies and individuals. More importantly, the Interpretation, by making clear references to the NSL, could hold companies and individuals — which deal often with personal information of its employees or customers, or which have the obligations under the NSL to properly administer and safeguard personal information — criminally liable for providing or obtaining personal information in a way inconsistent with the compliance requirements or obligations imposed by the NSL, e.g., failing to seek consent of data subjects or failing to ensure adequate security standards.

---

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

**Hui Xu**

hui.xu@lw.com  
+86.21.6101.6006  
Shanghai

**Gail E. Crawford**

gail.crawford@lw.com  
+44.20.7710.3001  
London

**Wei-Chun (Lex) Kuo**

lex.kuo@lw.com  
+852.2912.2511  
Hong Kong

**Andrea E. Stout**

andrea.stout@lw.com  
+44.20.7710.5843  
London

**Xuechu (Sean) Wu**

sean.wu@lw.com  
+86.21.6101.6013  
Shanghai

### You Might Also Be Interested In

[PRC's General Provisions of the Civil Law Enhance Personal Information Right and Data Protection](#)

[China Publishes Draft Measures Restricting Outbound Data](#)

[China Issues Its First Network Security Law](#)

---

*Client Alert* is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at [www.lw.com](http://www.lw.com). If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit <http://events.lw.com/reaction/subscriptionpage.html> to subscribe to the firm's global client mailings program.